Secretary of State

Oregon Audits Division

Oregon State Treasury

Cybersecurity Controls Audit

April 2021

Report 2021-12

Secretary of State Shemia Fagan
Audits Division Director Kip Memmott

Secretary of State
Oregon Audits Division

Executive Summary

Oregon State Treasury

Cybersecurity Controls Audit

Why This Audit is Important

» The Oregon State Treasury (OST), under the State Treasurer, acts as the state banker for the State of Oregon by maintaining all agency financial accounts and by investing some state funds, including the state's Trust Funds and bond fund proceeds.

» OST has over $118 billion in portfolio assets under its management. It processed 16 million transactions in 2019 worth $294 million.

» This audit assessed basic critical security controls and the information technology (IT) security management practices at OST.

» Cyberattacks are a growing concern for both the private and public sector. Recent breaches at Oregon state agencies have only escalated this concern. To protect against growing threats, IT management professionals should apply robust cybersecurity controls at various levels of infrastructure to protect IT resources.

What We Found

OST has a robust security management program that establishes a framework for assessing risk, developing, and implementing effective security procedures, and monitoring the effectiveness of those procedures. While the audit identifies several opportunities for OST to improve cybersecurity controls, the agency's focus, investment, and progress towards maintaining a secure IT environment is commendable and noteworthy. The audit identified the following areas for improvement:

1. OST's IT security plan does not detail how the agency currently addresses security for its information resources. Additionally, OST has not developed subordinate security plans that address how key applications are appropriately protected. (pg. 4)
2. Processes for updating inventory are largely manual and may not fully capture all hardware assets. Additionally, more controls are needed to ensure that only approved devices can connect to OST's network. (pg. 5)
3. OST lacks software policies and procedures, has an incomplete list of approved software, and has not implemented whitelisting to ensure only authorized software can be installed on agency systems. (pg. 6)
4. More work is needed to ensure that all devices are appropriately configured and monitored to ensure configuration settings remain appropriate. (pg. 7)
5. An additional independent time source should be added to ensure audit logs time stamps are accurate. (pg. 8)

Due to the sensitive nature of IT security and in accordance with Oregon state law and government auditing standards, we communicated details of the extent of the security weaknesses we identified to agency management in a confidential appendix.

What We Recommend

We made five recommendations to OST that include improving IT security plans and remedying weakness we identified in basic CIS Controls™. OST agreed with all of our recommendations. Their response can be found at the end of the report.

The Oregon Secretary of State Audits Division is an independent, nonpartisan organization that conducts audits based on objective, reliable information to help state government operate more efficiently and effectively. The summary above should be considered in connection with a careful review of the full report.

Introduction

Cyberattacks are a growing concern for both the private and public sector. Recent breaches at Oregon state agencies have only escalated this concern. In order to protect against growing threats, state agency leadership should ensure that information technology (IT) management professionals apply robust cybersecurity controls at various levels of infrastructure to protect their networks, servers, and user workstations for the agencies they oversee. State agencies utilize a variety of frameworks and standards with varying levels of detail to guide these efforts.

The Audits Division conducts cybersecurity audits to evaluate IT security risks and provide a high-level view of an agency's current state. We chose to use the Center for Internet Security's CIS Controls™, version 7.1. The CIS Controls™ are a prioritized list of 20 high-priority defensive actions that provide a starting point for enterprises to improve cyber defense. The controls are divided into three categories: basic, foundational, and organizational. This review includes the first six, the basic controls, which the Center for Internet Security, along with other security practitioners, defined as key controls that every organization should implement for essential cyber defense readiness.

In the following pages, we present the results as graphs depicting how many sub-controls in each control are not implemented, partially implemented, or fully implemented. This provides agency management, the Legislature, and others with responsibility for cybersecurity in the state with a snapshot of high-risk areas.

This audit does not consider an agency's risk appetite. Therefore, while these controls are considered basic by many security practitioners, agency management may choose not to fully implement a control if they determine within their strategic priorities that the cost of doing so outweighs the risk. In addition, while we generally considered controls that might mitigate some of the risks we identified, we did not perform a detailed review of potential compensating controls for each sub-control.

The Oregon State Treasury is exempt from Oregon's law unifying cybersecurity under Enterprise Information Services

In September 2016, the Governor signed Executive Order 16-13, unifying IT security functions for the majority of state agencies in order to protect and secure information entrusted to the State of Oregon. The order directed executive branch agencies to consolidate security functions into the Office of the State Chief Information Officer, now known as Enterprise Information Services (EIS). The passage of Senate Bill 90 in June 2017 made the order permanent.

However, multiple state agencies were specifically excluded. These agencies include:

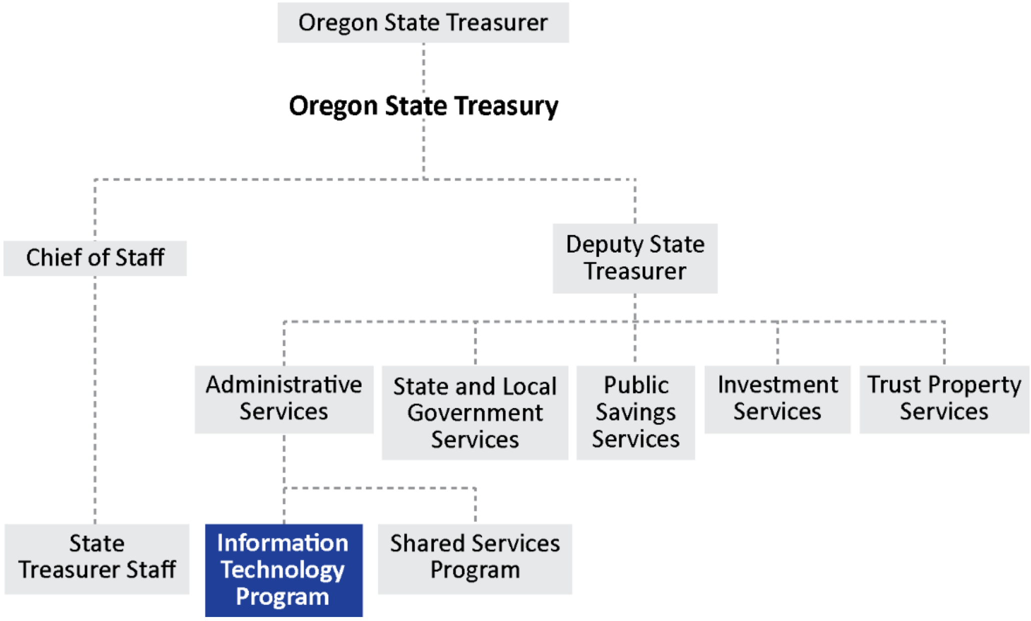
- Secretary of State;
- Oregon State Treasury (OST);
- Attorney General, including the Department of Justice;
- Oregon State Lottery; and
- public universities listed in ORS 352.002.

As such, while Senate Bill 90 resulted in the transfer of 30 security-related positions from state agencies to EIS, OST retained all its IT security staff and remained solely responsible for achieving and sustaining optimum levels of information confidentiality, integrity, and availability across the platforms it uses.

OST provides financial stewardship for Oregon

Article VI, Section 1 of the Oregon Constitution created OST, which is directed by a statewide elected official, the State Treasurer. State law establishes the powers and duties of the Treasurer and designates the incumbent as the investment officer for the Oregon Investment Council, which is responsible for establishing the state's investment policy. The State Treasurer also serves on the State Land Board and chairs the State Debt Policy Advisory Commission, among other duties and responsibilities.

The mission of the agency is to provide financial stewardship for Oregon. The State Treasurer acts as the banker for the State of Oregon by maintaining all state agency financial accounts and by investing state funds not needed to meet current expenditure demands, including the state's trust funds and bond fund proceeds. OST has a 2021-23 proposed budget of over $128 million and manages a portfolio of over $118 billion as of year-end 2020. In 2019 OST processed 16 million financial transactions worth $294 million.



OST operates five service areas:

- State and Local Government Financial Services: Provides banking and short-term investment services to all state agencies, most public universities, and services to local governments. Also provides central coordination for, and issuance of all Oregon state agency and authority bonds.

- Public Savings Services: Oversees several public "defined contribution" investment programs, which advance the connected policy goals of increasing individual savings and quality of life, and reducing long-term government costs.

- Investment Services: Manages funds and trust funds in accordance with policies and asset allocation targets set by the Oregon Investment Council.

- Trust Property Services: Acts as the depository of record for unclaimed and presumed abandoned property and funds.

- Administrative Services: Provides the support needed to ensure the State Treasury and all Treasury programs have the administrative infrastructure, operational resources, and technology necessary to fulfill their mission and statutory requirements.

The agency procures budget and accounting services from the Department of Administrative Services.

OST IT Services is located within Treasury's Administrative Services

Information Technology Services is responsible for IT within OST and is located within Treasury's Executive Services Division. It supports Treasury by providing a secure and stable network as well as application support for both in-house and external systems. The IT Services proposed budget for the 21-23 biennium is $14.7 million and includes 34 positions.

As part of its long-term strategic plan, OST has made information security a top priority and has requested increased funding for cybersecurity within its 2021-23 budget. The purpose of this request is to help ensure financial transactions and business-critical data entrusted to OST are protected from evolving and emerging information security threats. OST plans to use the additional budgeted funds to mature its information security program and meet federal, state, and local government requirements by continuing to improve protections in line with current financial industry best practices.

OST has also requested one additional position and related funds to purchase and implement additional security tools and services to help improve the organization's security posture and meet the growing information security needs of OST and its customers.

Information Technology Services consists of four teams:

- Technical Services Delivery
- Infrastructure Services
- Information Security Services
- Application Development Services

Audit Results

Our review determined that OST has a robust security management program that establishes a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of those procedures. While the audit identifies several opportunities for OST to improve cybersecurity controls, the agency's focus, investment, and progress towards maintaining a secure IT environment is commendable and noteworthy. However, our review also identified some areas where OST should improve cybersecurity controls.

We found that OST has implemented or partially implemented 44 of 47 basic sub-controls reviewed as part of this audit. Additionally, while not reviewed as part of this audit, we noted that OST reports to have made significant progress in implementing additional advanced cybersecurity controls recommended by the Center for Internet Security. This progress is largely due to OST executive management prioritizing cybersecurity and providing full support to the efforts of Information Technology Services.

We considered the risks posed by publicly releasing any information related to security findings. As part of our consideration, we balanced the need for stakeholders, such as the Legislature, to be informed on critical or systemic IT security issues affecting the State against the need to protect the agency from cybersecurity threats. Consequently, in accordance to ORS 192.345 (23) and generally accepted government auditing standards, we excluded some details of the security weaknesses from this public report and provided them to agency management in a confidential appendix.

OST has a robust and increasingly mature security management and compliance program that can benefit from further improvements

Effective security management requires agencies to have policies, plans, and procedures that describe the management program and cover all major systems, facilities, and applications. Detailed roles and responsibilities should be clearly defined. Specifically, agencies should:

- Periodically assess and validate risks;
- Document and implement security control policies and procedures;
- Implement and monitor effective security awareness trainings;
- Remediate information security weaknesses; and
- Ensure external third-party activities are adequately secured.

We determined that OST has a robust security management and compliance program that includes periodic risk assessments, robust security control policies and procedures, security awareness training, identification and remediation of security weaknesses, and appropriate third-party security and monitoring.

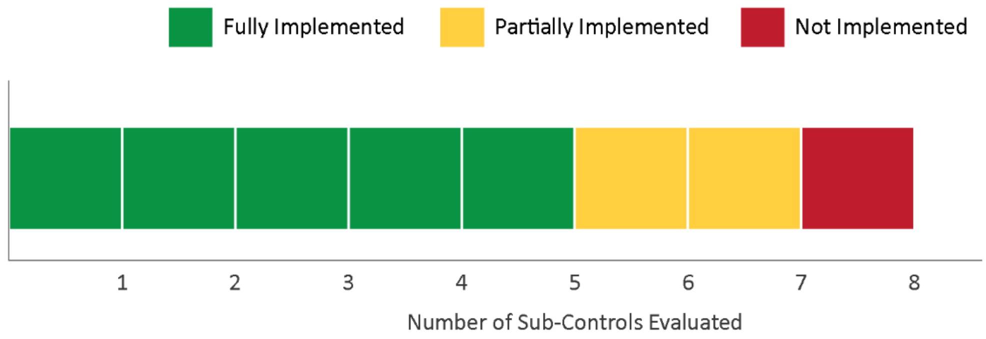
However, while OST has developed an IT Security Plan, we found the plan is largely focused on the agency's future state of IT security; it does not address how OST currently achieves security of its information resources. Additionally, OST has not developed subordinate security plans to address how key applications are appropriately protected against unauthorized use, disclosure, or modification.

While the plan itself is lacking these details, this does not suggest that appropriate controls are not in place as demonstrated by the following limited controls review. However, without a well-documented IT Security Plan that includes the current state of IT security controls, along with subordinate application security plans, existing controls and responsibilities may be unclear, misunderstood, improperly implemented, or inconsistently applied.

CIS Controls Review

For this audit, we evaluated the implementation level of the agency's cybersecurity control environment against the top six CIS Controls™ and their associated sub-controls. We evaluated each sub-control to provide an assessment of the agency's overall cybersecurity implementation. The charts below illustrate the number of controls evaluated for each control objective, and whether that control is fully implemented, partially implemented, or not implemented.

CIS Control™ 1: Inventory of Authorized and Unauthorized Devices

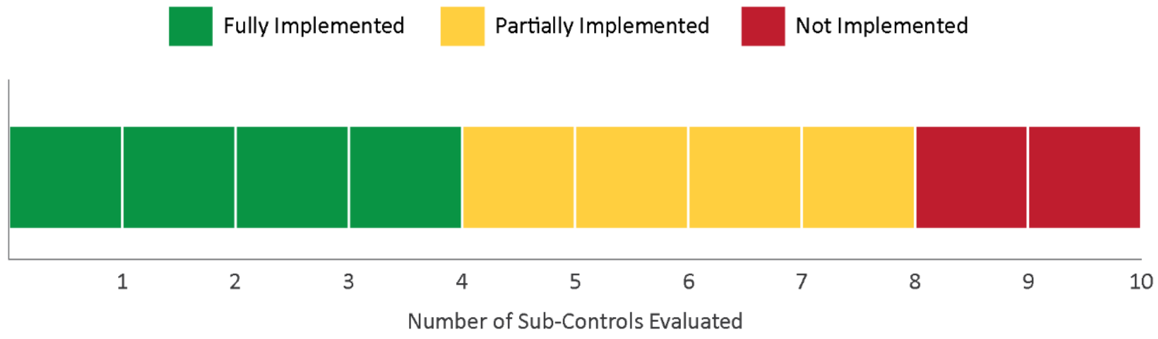


We evaluated OST's processes to identify network devices, maintain an updated inventory of hardware devices, and ensure only approved devices can connect to the network. We found that OST has implemented or partially implemented most of the recommended controls over asset inventory.

OST utilizes multiple applications and tools to track and monitor systems such as workstations, laptops, printers, servers, and network devices. However, OST's process for updating inventory is largely manual and may not fully capture all its hardware assets. Additionally, more controls are needed to ensure that only approved devices can connect to its network.

Any new device introduced to an agency's network may introduce vulnerabilities. Ensuring only authorized devices have access to information on the agency's network allows IT professionals to identify and remediate vulnerabilities by implementing proper security controls. However, without a clear understanding of which devices are on the network, the agency cannot ensure proper controls are in place for those devices. Additionally, without an accurate, up-to-date inventory of authorized hardware, the agency cannot actively manage and monitor all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.

CIS Control™ 2: Inventory of Authorized and Unauthorized Software

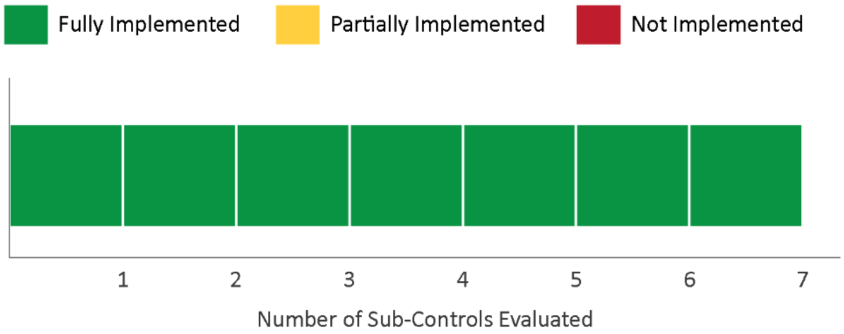


We evaluated OST's process to document approved software, segregate high-risk software, and identify software installed on its systems. We determined OST has tools in place to identify and track software installed on devices connected to its network. However, work remains to ensure only authorized and supported software is installed on agency systems. Among other weaknesses, we noted that OST lacked policies and procedures, had an incomplete list of approved software, and had not implemented whitelisting to ensure only authorized software can be installed on agency systems.

Controls should be established by implementing software whitelisting, automating software inventory, and monitoring software installations on all systems. Organizations should maintain an inventory of software installed on their computer systems similar to the inventory of its hardware assets. If an agency does not have a complete, accurate, and up-to-date list of the software authorized to be on its systems, it cannot ensure effective controls are in place to update installed software. Attackers continuously scan targeted organizations looking for vulnerable versions of software to exploit. Software that is no longer supported by its vendor is especially vulnerable to this type of attack, as patches are no longer developed to remediate vulnerabilities.

In addition, without an inventory of system software, an agency may be unable to identify unauthorized software on its information systems, such as malicious software or software with known vulnerabilities. Attackers can exploit systems with malicious or vulnerable software to gain unauthorized access to the agency's data or disrupt operations. Workstations are also more likely to be either running software that is unneeded for business purposes, which could introduce potential security flaws, or running malware introduced by an attacker after a system is compromised.

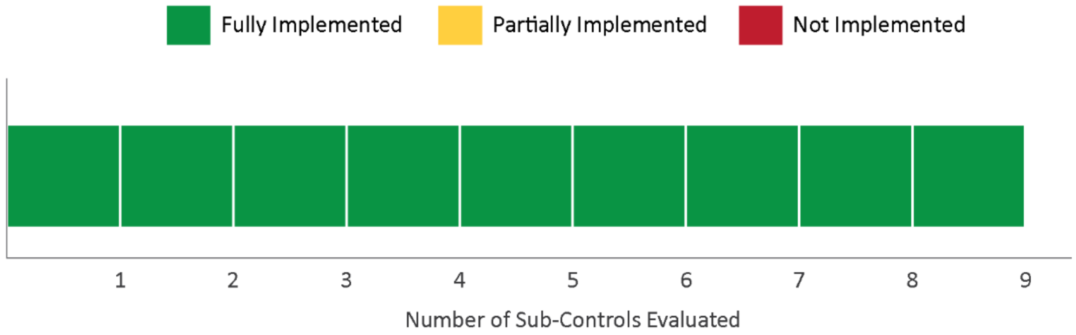
CIS Control™ 3: Continuous Vulnerability Assessment and Remediation



We determined that OST has fully implemented controls to ensure that vulnerabilities are identified and timely remediated or patched. This includes performing authenticated vulnerability scanning using appropriate scanning tools, protecting dedicated assessment accounts, deploying automated operating system and application patch management tools, and comparing back-to-back vulnerability scans with an appropriate risk-rating process. Additionally, we tested 10% of OST's endpoints and found that all were appropriately patched and up-to-date.

Organizations should be continuously engaged in identifying, remediating, and minimizing security vulnerabilities to ensure their assets are safeguarded. Attackers commonly exploit IT systems that have not been patched with security updates or have other known vulnerabilities. This could compromise the confidentiality, integrity, or availability of agency data. By scanning the network for known vulnerabilities, an agency can identify and prioritize software patching and other remediation activities to ensure these known risks are controlled.

CIS Control™ 4: Controlled Use of Administrative Privileges

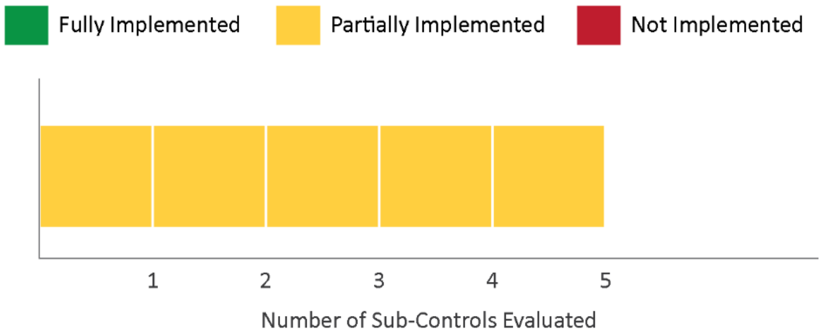


We assessed OST's processes to grant privileged access accounts, log and monitor login activity, and to establish robust authentication procedures.[1] We found the agency has strong processes and procedures for granting, reviewing, and terminating access for privileged accounts. Additionally, we found that the agency has robust monitoring of the use of these accounts, including maintaining an inventory of accounts, removal of default passwords, unique password requirements, logging and alerts of account usage, and limits on the use of script tools.

We reviewed OST's privileged accounts and policies to determine if access was set up, monitored, and reviewed on a periodic basis using the principle of least privilege.[2] Overall, we found that OST has appropriate processes and procedures, but processes to grant, review, and terminate third-party vendor access needs better tracking.

Management of privileged users should ensure only authorized users are able to perform administrative functions on the agency's information systems. While some users may have authorization to read, edit, or delete data based on their job duties, other users have access to advanced functions such as system control, monitoring, or administrative functions. Actions performed under these administrative accounts may have critical effects on the agency's systems. Therefore, use of accounts with these privileges should be effectively controlled by management, including implementing controls to segregate, manage, and monitor use of these accounts.

CIS Control™ 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers



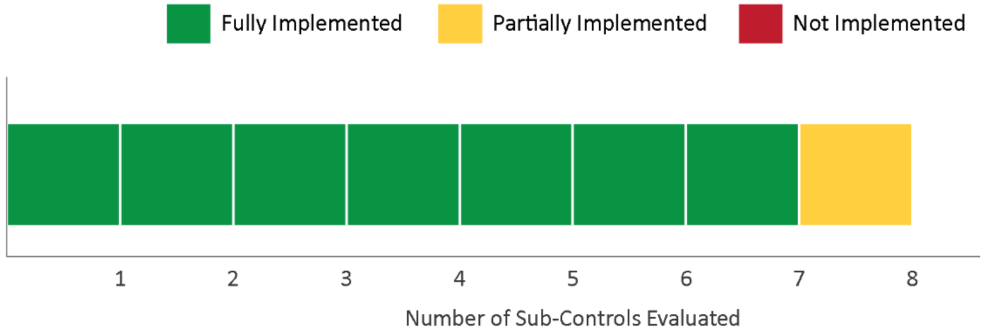
We evaluated OST's processes to document and safeguard baseline configurations, deploy secure configurations, and monitor configurations on its network. We determined OST has

[1] Privileged access refers to the ability of some users to take actions that may affect computing systems, network communications, or the accounts, files, data, or processes of other users. Privileged access implies greater access than the average end user has.
[2] Least privilege is a principal that states that users should have the least amount of privileges (access to services) necessary to perform their duties.

established secure baselines for most servers, network devices, and workstations, but more work is needed to ensure that all devices are appropriately configured and monitored to ensure settings remain appropriate.

Organizations should have processes in place to ensure hardware and software are securely configured. This should include verifying that default configurations align with business and security needs so that agency systems are not left vulnerable to attack. The agency should also have configuration management processes in place that address implementing secure system control features at the initiation of the system lifecycle. Furthermore, an organization should ensure configurations remain secure as modifications are made to the system. Baselines should be documented so agency personnel can effectively monitor actual configurations to ensure they align with established baselines. Also, policies and procedures should be in place that address how configuration baselines are managed.

CIS Control™ 6: Maintenance, Monitoring, and Analysis of Audit Logs



We reviewed OST's processes for collecting, managing, and analyzing audit logs of events that could help the agency detect, understand, or recover from an attack. We found that OST has fully implemented controls over the maintenance, monitoring, analysis of audit logging. This includes enabling detailed audit logs for all network devices and endpoints, ensuring adequate log storage, centralized log management, reviewing logs on a regular basis, establishing appropriate log alerts, and procedures for regularly tuning the log management system. However, OST should take steps to ensure the agency has an adequate number of independent time sources to further ensure audit logs time stamps are accurate.

Robust logging and log monitoring processes allow organizations to identify and understand inappropriate activity and recover more quickly from an attack. Deficient logging may allow attackers and malicious activity to go undetected for extended periods. Moreover, attackers know that many organizations rarely review log information, allowing attacks to go unnoticed. Agencies should ensure that information systems record the type, location, time, and source of events that occur. Additionally, processes should be established to ensure these logs are periodically reviewed so the agency can identify inappropriate or unusual activity and remediate security events.

Recommendations

To improve critical cybersecurity controls, we recommend OST:

1. Update IT security plans to include all necessary elements, including the current state of IT security and subordinate security plans.
2. Remedy weaknesses with CIS Control #1 — Hardware Inventory — by fully automating asset discovery and inventory and fully implementing hardware authentication controls.
3. Remedy weaknesses with CIS Control #2 — Software Inventory — by updating documentation of approved software, ensuring software is supported by its vendor, and implementing software whitelisting.
4. Remedy weaknesses with CIS Control #5 — Secure Configurations — by establishing security configuration for all servers and network devices and strengthening configuration monitoring and alerts to ensure all changes to configuration are authorized and appropriate.
5. Remedy weaknesses with CIS Control #6 — Audit Logs — by establishing an adequate number of independent time sources to ensure audit logs time stamps are accurate.

Objective, Scope, and Methodology

Objective

Our audit objective was to determine the extent to which OST has implemented an appropriate IT security management program, as well as selected controls from the Center for Internet Security's CIS Controls™, version 7.1.[3] These controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices to help protect systems and networks from the most common attacks.[4]

Scope

The scope of this work included a review of security management and the first six of the 20 CIS Controls™ in place at OST during the third and fourth quarters of 2020. Cybersecurity experts generally agree that these six "basic" controls should be implemented by all organizations for cyber defense readiness.

The following internal control principles were relevant to our audit objective:

- Security Management
  - Establish a security management program;
  - Periodically assess and validate risks;
  - Document and implement security control policies and procedures;
  - Implement effective security awareness and other security-related personnel policies;
  - Monitor the effectiveness of the security program;
  - Effectively remediate information security weaknesses; and
  - Ensure that activities performed by external third parties are adequately secure.
- Inventory and Control of Hardware Assets
  - Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
- Inventory and Control of Software Assets
  - Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that all unauthorized and unmanaged software is found and prevented from installation or execution.
- Continuous Vulnerability Management
  - Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
- Controlled Use of Administrative Privileges
  - The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
  - Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a

[3] Center for Internet Security CIS Controls

[4] Defense-in-depth refers to the application of multiple countermeasures in a layered or stepwise manner to achieve security objectives.

rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.
- Maintenance, Monitoring and Analysis of Audit Logs
    - Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Deficiencies with these internal controls were documented in the audit results section of this report. Other elements of internal control were not deemed necessary to achieve the objective of the audit and were excluded from scope.

Methodology

To assess whether management has established policies and implemented controls to stop cyberattacks that may target the agency, we:

Reviewed:

- IT Policies and procedures;
- External IT risk assessments and audits;
- Hardware asset inventory lists;
- Software asset inventory lists;
- Privileged user access lists;
- Network diagrams.

Observed:

- Configuration settings;
- Vulnerability scan results;
- Software installed on workstations;
- IT processes and ad hoc activities.

Interviewed:

- IT staff;
- IT managers;
- Agency Director of IT;
- Agency leadership.

We considered the risks posed by publicly releasing any information related to security findings. As part of our consideration, we balanced the need for stakeholders, such as the Legislature, to be informed on critical or systemic IT security issues affecting the State against the need to protect the agency from cybersecurity threats. Consequently, in accordance to ORS 192.345 (23) and generally accepted government auditing standards, we excluded some details of the security weaknesses from this public report and provided them to agency management in a confidential appendix.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis to achieve our audit objective.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of OST during the course of this audit.

OREGON
STATE
TREASURY

Tobias Read
Oregon State Treasurer

Michael Kaplan
Deputy State Treasurer

April 8, 2021

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled Oregon State Treasury – Cybersecurity Controls Audit.

We would like to thank the Secretary of State's staff assigned to the Cybersecurity Controls Audit for their courtesy, professionalism, and expertise during the audit. It was evident early in the process that we have share a common goal of protecting agency information technology assets with standards-based processes and controls.

For our work at Treasury, cybersecurity is critically important to the successful and effective delivery of financial services to the State of Oregon. Treasury is committed to continuing the work and investments recognized in the audit that have advanced and improved our cybersecurity posture. Further, we will prioritize remediating the issues identified in the audit and expanding our long-term planning and ensure remediated efforts are aligned with the current Statewide Information and Cyber Security Standards. We look forward to incorporating your recommendations into our Information Security Program.

OST's responses to each recommendation in the audit are listed below. Should you have any additional questions regarding the information provided, please do not hesitate to contact Michael Kaplan, Deputy State Treasurer, at Michael.kaplan@ost.state.or.us.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 1</b>
Update IT security plans to include all necessary elements, including the current state of IT security and subordinate security plans.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>June 2023</td><td>Alain Bouit</td></tr>
</table>

Narrative for Recommendation 1

Treasury will update our security plan to include system security plans for major applications and systems. We anticipate that we will implement this documentation and associated policy and procedures by the end of 21-23 biennium.

RECOMMENDATION 2
Remedy weaknesses with CIS Control #1 — Hardware Inventory — by fully automating asset discovery and inventory and fully implementing hardware authentication controls.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 2023	Alain Bouit

Narrative for Recommendation 2

Treasury is in the process of implementing technology designed to detect, alert, and manage authorized and unauthorized devices that plugs into the network. Policies and procedures are being crafted to ensure only authorized devices connect to Treasury's network. Full implementation of the technology, policy, and procedures is anticipated to be completed by the end of 21-23 biennium.

RECOMMENDATION 3
Remedy weaknesses with CIS Control #2 — Software Inventory — by updating documentation of approved software, ensuring software is supported by its vendor, and implementing software whitelisting.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 2023	Alain Bouit

Narrative for Recommendation 3

Treasury is currently implementing technology, policies, and procedures to ensure that only approved software is installed and can run on agency systems. Our target for completion is by the end of 21-23 biennium.

RECOMMENDATION 4
Remedy weaknesses with CIS Control #5 — Secure Configurations — by establishing security configuration for all servers and network devices and strengthening configuration monitoring and alerts to ensure all changes to configuration are authorized and appropriate.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 2023	Alain Bouit

Narrative for Recommendation 4

Treasury will continue to complete our configuration management project and finish the work of crafting policies and procedures to ensure all servers and network devices are securely configured and properly managed. The configuration management project is targeted for completion by end of the 21-23 biennium.

Treasury will complete ongoing efforts required for configuration management, threat and anomaly detection services, and management of critical elements of application security. As part of the process to address the issues, and in accordance with our wider IT plan to strengthen effective systems management, Treasury has submitted a budget request for one permanent security analyst position in the 21-23 legislative session.

RECOMMENDATION 5
Remedy weaknesses with CIS Control #6 — Audit Logs — by establishing an adequate number of independent time sources to ensure audit logs time stamps are accurate.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	June 2023	Alain Bouit

Narrative for Recommendation 5

Treasury will implement additional, independent time sources as part of the building resiliency project, intended to be completed by the end of the 21-23 biennium.

Thank you again for your thoughtful engagement and comments.

Please contact Michael Kaplan, Deputy State Treasurer, at Michael.kaplan@ost.state.or.us with any questions.

DocuSigned by:
Michael Kaplan
836AC54B913A401...

Sincerely,
Michael Kaplan,
Deputy Treasurer

Audit Team

Teresa Furnish, CISA, Audit Manager

Matthew Owens, MBA, CISA, Principal Auditor

Shelia Faulkner, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits